Notice of Allowability	Application No.	Applicant(s)	
	10/655,387	RADATTI, PETER V.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an Examiner initiated interview on 11/22/10*.

2. ☒ The allowed claim(s) is/are *1-35 and 37*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11/22/10* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Michael Pyzocha/ Primary Examiner, Art Unit 2437	

DETAILED ACTION

1. Amendment filed 10/08/2010 has been received and considered.

2. Claims 1-37 are pending.

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Frank Bonini (Reg. No. 35,452) on 11/22/2010.

The application has been amended as follows:

Claim 1. (Currently amended) An apparatus for processing code comprising: at least one electronic device component for intercepting, examining and controlling code that is being communicated as a code stream on a communications channel, said electronic device component being provided with a protocol parser capable of discriminating among different protocols implemented on top of the transport layer; and, a proscribed code scanner; whereby said protocol parser intercepts instant messaging or peer-to-peer code on a communications channel and transmits said code for review by said proscribed code scanner, said protocol parser being provided to parse protocols on top of the transport layer; wherein said apparatus is configurable to process multiple code streams created when more than one communications channel is opened;

the apparatus including at least one kernel module that is linked to a number of path names and remains operable, and wherein a ~~said~~ kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising instant messaging or peer-to-peer code, wherein said interception is based on one or more of code based or port based interception.

Claim 2. (Original) An apparatus as in claim 1 further comprising a translation means whereby said translation means translates said code to authorized program parameters.

Claim 3. (Original) An apparatus as in claim 1 further comprising a protocol scanner, whereby said protocol parser transmits said instant messaging or peer-to-peer code to said proscribed code scanner through said protocol scanner.

Claim 4. (Original) An apparatus as in claim 1 whereby said proscribed code scanner further comprises a scanning means and an indicator means.

Claim 5. (Original) An apparatus as in claim 1 further comprising a certification means.

Claim 6. (Original) An apparatus as in claim 4 whereby said indicator means provides an indication of the presence of proscribed code after scanning said intercepted code.

Claim 7. (Original) An apparatus as in claim 1, whereby said proscribed code scanner comprises a malicious code scanner.

Claim 8. (Original) An apparatus as in claim 1, wherein said protocol parser further comprises a configuration means for configuring interception parameters.

Claim 9. (Currently amended) An apparatus for processing code comprising: at least one electronic device component for intercepting, examining and controlling code that is being communicated as a code stream on a communications channel, said electronic device component being provided with a protocol parser capable of discriminating

among different protocols implemented on top of the transport layer; and, a proscribed code scanner; whereby said protocol parser intercepts short messaging code from said code stream on a communications channel and transmits said code for review by said proscribed code scanner and said protocol parser being provided to parse protocols on top of the transport layer;

the apparatus including at least one kernel module that is linked to a number of path names and remains operable, and wherein a ~~said~~ kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising ~~instant~~ short messaging, wherein said interception is based on one or more of code based or port based interception.

Claim 10. (Original) An apparatus as in claim 3, wherein said protocol scanner further comprises a configuration means for configuring interception parameters.

Claim 11. (Currently amended) An apparatus for processing code comprising: at least one electronic device component for intercepting, examining and controlling code that is being communicated as a code stream on a communications channel, said electronic device component being provided with a protocol parser capable of discriminating among different protocols implemented on top of the transport layer; a protocol scanner; and, a proscribed code scanner comprised of a scanning means and an indicator

means; whereby said protocol parser intercepts instant messaging or peer-to-peer code on a communications channel and transmits said code to said proscribed code scanner through said protocol scanner, said protocol parser being provided to parse protocols on top of the transport layer,

the apparatus including at least one kernel module that is linked to a number of path names and remains operable, and wherein a kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising instant messaging or peer-to-peer code, wherein said interception is based on one or more of code based or port based interception.

Claim 12. (Original) An apparatus as in claim 1, further comprising a decryption component, whereby said protocol parser intercepts said instant messaging or peer-to-peer code being transmitted through said communications channel and transfers said code to said decryption component for decryption and scanning by said proscribed code scanner.

Claim 13. (Original) An apparatus as in claim 12, further comprising an SSL decryption component.

Claim 14. (Original) An apparatus as in claim 12, further comprising an S/MIME decryption component.

Claim 15. (Original) An apparatus as in claim 1, further comprising an encryptor, wherein said code, after being processed by said proscribed code scanner, may be encrypted by said encryptor.

Claim 16. (Original) An apparatus as in claim 12, further comprising an encryptor, wherein said code, after being processed by said proscribed code scanner, may be encrypted by said encryptor.

Claim 17. (Currently amended) An apparatus for processing code comprising: at least one electronic device component for intercepting, examining and controlling code that is being communicated as a code stream on a communications channel, said electronic device component being provided with a protocol parser capable of discriminating among different protocols implemented on top of the transport layer; a proscribed code scanner; a protocol scanner; a decryption component, whereby said protocol parser intercepts instant messaging or peer-to-peer code on a communications channel and transfers said code to said decryption component for decryption and scanning by said proscribed code scanner, said protocol parser being provided to parse protocols on top of the transport layer.

the apparatus including at least one kernel module that is linked to a number of path names and remains operable, and wherein a kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising instant messaging or peer-to-peer code, wherein said interception is based on one or more of code based or port based interception.

Claim 18. (Currently amended) A method for processing code comprising: providing a computing component with storage media, and configuring the storage media with software for implementing the following: intercepting instant messaging or peer-to-peer code that is being communicated as a code stream on a communications channel; parsing said code; and, scanning said code for the presence of proscribed code; and, providing an indicator for the presence of said proscribed code, wherein parsing said code comprises discriminating among different protocols;

wherein the computing component includes at least one kernel module that is linked to a number of path names and remains operable, and wherein a kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising instant messaging or peer-to-peer code, wherein said interception is based on one or more of code based or port based interception.

Claim 19. (Original) A method as in claim 18 further comprising translating said code to authorized program parameters.

Claim 20. (Original) A method as in claim 18 further comprising said code.

Claim 21. (Original) A method as in claim 18 further comprising returning said code to said communication channel if said indicator is negative.

Claim 22. (Original) A method as in claim 18 further comprising transferring said code to another communication channel.

Claim 23. (Original) A method as in claim 18 further comprising further indicating the presence of said proscribed code if said indicator is positive.

Claim 24. (Original) A method as in claim 18 wherein intercepting said code further comprises intercepting the code according to configured parameters.

Claim 25. (Original) A method as in claim 18 wherein scanning said code for the

presence of proscribed code further comprises scanning said code for the presence of malicious code.

Claim 26. (Original) A method as in claim 18 further comprising decrypting said code.

Claim 27. (Original) A method as in claim 26 further comprising reencrypting said code if said indicator is negative.

Claim 28. (Original) A method as in claim 18 further comprising encrypting said code.

Claim 29. (Original) A method as in claim 26 wherein decrypting said code is preceded by intercepting said code prior to decrypting said code.

Claim 30. (Original) A method as in claim 26 wherein said code is secured through SSL encryption.

Claim 31. (Original) A method as in claim 26 wherein said code is secured through S/MIME encryption.

Claim 32. (Original) A method as in claim 26 further comprising the step of: reencrypting said code if said indicator is negative.

Claim 33. (Original) A method as in claim 26 further comprising providing a separate system inserted in said communications channel, and with at least one of said steps of intercepting said code; decrypting said code; scanning said code for the presence of proscribed code, and providing an indicator for the presence of said proscribed code, occurring on said separate machine.

Claim 34. (Currently amended) A method for processing code comprising: providing a computing component with storage media, and configuring the storage media with software for implementing the following: intercepting short messaging ~~instant messaging or peer-to-peer~~ code that is being communicated as a code stream on a communications channel; parsing said code; scanning said code for the presence of proscribed code; and, providing an indicator for the presence of said proscribed code, wherein parsing said code comprises discriminating among different protocols;

wherein the computing component includes at least one kernel module that is linked to a number of path names and remains operable, and wherein a kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising short messaging, wherein said interception is based on one or more of code based or

port based interception.

Claim 35. (Currently amended) A method for processing code comprising: providing a computing component with storage media, and configuring the storage media with software for implementing the following: intercepting instant messaging or peer-to-peer code that is being communicated as a code stream on a communications channel; decrypting said code; parsing said code; scanning said code for the presence of proscribed code; and, providing an indicator for the presence of said proscribed code, wherein parsing said code comprises discriminating among different protocols;

wherein the computing component includes at least one kernel module that is linked to a number of path names and remains operable, and wherein a kernel is configured to operate to intercept code streams when an application that the kernel module is linked to is opened, wherein said application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream;

wherein the kernel module is configured to intercept at least code comprising instant messaging or peer-to-peer code, wherein said interception is based on one or more of code based or port based interception.

Claim 36. (Canceled)

Claim 37. (Previously presented) The method as in claim 30, wherein parsing said code is accomplished with a parser, and wherein the method includes intercepting with

said parser a request from one or the other of an original client and an original server for an SSL transfer, creating with said parser a new SSL server that communicates with said client and a new SSL client that communicated with said server, and intercepting with said SSL client and said SSL server communications that occur between said original client and said original server.

Double Patenting

4. The nonstatutory double patenting rejections have been withdrawn based on the filed amendment. The patented claims and the prior art fail to render the present claims obvious and therefore the double patenting has been withdrawn.

Allowable Subject Matter

5. Claims 1-35 and 37 are allowed.

6. The following is an examiner's statement of reasons for allowance: The prior art generally teaches the use of kernel modules linked to path names where a kernel intercepts code, but the prior art fails to explicitly disclose the application calls the kernel to insert a kernel module in the code stream, and wherein said kernel module intercepts code passing in the stream; wherein the kernel module is configured to intercept at least code comprising instant messaging or peer-to-peer code, wherein said interception is based on one or more of code based or port based interception when in combination with the remaining claim limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Shealy teaches monitoring data streams using a kernel.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Michael Pyzocha/
Primary Examiner, Art Unit 2437